



UNITED STATES PATENT AND TRADEMARK OFFICE

AMT

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/496,065	02/01/2000	N. Asokan	SZ998-041	5668

7590 01/13/2005

Anne Vachon Dougherty Esq
IBM Corp
3173 Cedar Rd
Yorktown Heights, NY 10598

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/496,065	ASOKAN ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 August 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 9-26 and 30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 9-26 and 30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 8/23/04 was received and considered.
2. Claims 9-26 & 30 are pending.

Response to Arguments

3. In light of applicant's amendments to the claims, the rejections of claims 9-11 and 29 under 35 U.S.C. §112 are withdrawn.
4. Applicant's arguments filed 8/23/04 have been fully considered but they are not persuasive. The rejections of claims 9-26 & 30 are maintained. Applicant's arguments (p. 9, ¶2 – p. 11, ¶2) are directed to the Merritt patent only, rather than to specific claims. The rejections based on the Merritt patent will be addressed below with respect to the independent claim 9, and rejections based on the combination of Merritt and Manduley claims 12 & 30 (It is noted that applicant has amended claim 30 "to parallel the language of Claim 12" and is "defended as if the Examiner rejected claim 30 using the same art used to reject Claim 12").

Regarding claim 9, Merritt discloses a server/host with a communication component/communication line (col. 2, lines 48-64) for communication along a first trusted connection with a terminal (Fig. 2) and a second trusted connection with said user device (col. 6, lines 21-22) (card sends data, possibly with PIN, to host through ATM), receiver means for receiving at least one authentication request from said terminal (Fig. 3, #310, 315), at least one authentication component/comparator (Fig. 1) for verifying the authenticity of the terminal (col. 4, lines 58-64), and a message generation component for generating at least one authenticity output message/PSP for delivery to said user input device along said second connection (from

Art Unit: 2134

host to ATM screen). The claim is directed to a server with functionality that has a message generation component, which is disclosed in Merritt. The user input device is the combined presentation module, keyboard and card reader, whereas the terminal represents the receiving and processing circuitry in Fig. 1.

Regarding applicant's arguments to claims 12 and amended claim 30, Merritt discloses a server/host authenticating a terminal/ATM (Fig. 3, #315), establishing a first authenticated trusted connection upon success of said authenticating (Fig. 3, #315) which also establishes a second trusted connection between the user/device and the server. Merritt further discloses the server authenticating it to the device/user by providing a terminal authenticity message/PSP sent to the terminal to be displayed to the user (second trusted connection) (Fig. 3, #380). Merritt lacks sending the authenticity to the device. The Manduley reference teaches that smart cards are useful in secure transactions, particularly as an electronic purse (as would be used at an ATM) (col. 1, lines 11-29). Manduley also teaches that exchanging messages between a user and a smart card is useful to make sure the correct user is using the smart card (col. 2, lines 7-23 & col. 1, lines 41-56). More specifically, Manduley teaches that the smartcard contains an LCD display that will, at the request of the server/issuing authority, display a message to the user (col. 3, lines 11-16, lines 47-58). This message can be a message requesting the user to enter a response (col. 3, lines 47-58) to authenticate the user (col. 4, lines 7-15). Manduley's teaching can be applied to the Merritt invention, wherein a smart card is used to interact with the bank and the authenticity output message is received from the server, via a second connection, and displayed on the LCD display of the smart card. Therefore, the rejection is maintained.

Applicant's response (p. 11, ¶3 & p. 12, ¶1) argues that the server provides terminal authentication information directly to the user device (Claims 9-26 & 30). This specific limitation does not appear in the amended claims and was cancelled from claim 9. It is noted that this features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant's response (p. 11, ¶3 & p. 12, ¶1) argues that claim 18 “further expressly recites that the user device provides user-specific information to the terminal, after receiving terminal authentication information from the server, for use by the terminal in dynamically creating the authenticity output message.” The Examiner notes that neither the “after receiving terminal authentication information from the server” nor “for use by the terminal in dynamically creating the authenticity output message” is recited in the claim.

Applicant's response (p. 12, ¶1) argues that the Merritt patent does not teach that “a user device authenticate a user”. The Examiner notes that this feature is not in the claims. The claims recite the limitation “the device requesting that the user authenticate himself” (Claim 20), which is taught by Manduley (col. 3, lines 47-58).

5. Applicant's response (p. 12, ¶2) argues that the Manduley patent is cited for teaching a method for assuring that the user is actually in possession of the card and that “that is NOT what is being claimed.” The fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). Further, the result of the Manduley teaching is only cited for motivation for

Art Unit: 2134

combining the features stated in the Office Action with the Merritt reference; the motivation is not purported to read on applicant's claims.

6. Applicant's response (p. 13, lines 14-23) argues that "neither Manduley nor Merritt teaches that a terminal authentication message be communicated directly to a user along a connection between the user and the server, without also communicating the message along the connection between the terminal and the server" (emphasis added). In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., specifically, the previous emphasized limitations) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

7. Applicant's response (p. 14, ¶1) argues that the combination of Merritt and Manduley would not arrive at the invention as claimed because it would create a system where the user is first authenticated to the terminal and then the terminal would proceed to seek its own authentication from the server. Applicant is reminded that the ordering, unless explicit, is not read from the claims; the ordering of the server authenticating the terminal and the server authenticating itself to the device is not explicit. Further, the user authentication in the Merritt patent happens when the user enters his/her PIN, which occurs after the terminal displays the authentication message (col. 6, lines 21-35).

8. Applicant's response (p. 15, ¶1) argues that Schneier does not render the invention obvious, because the combination of Merritt and Manduley does not "include communication of terminal authentication along a connection between a server and a user device and not along a

Art Unit: 2134

different connection between the terminal and the server". The previously underlined limitation is not presented in the claim. Further, the terminal communication between a server and a user device is presented in Manduley (col. 3, lines 47-58).

9. Applicant's response (p. 15, ¶2) argues that the introduction of Lessin would teach away from the claimed invention because it would require the user enter his PIN in an un-trusted terminal. However, the user authentication in the Merritt patent happens when the user enters his/her PIN, which occurs after the terminal displays the authentication message (col. 6, lines 21-35). Further, applicant states that claim 20 requires "the server first send terminal authentication information directly to the user, apart from the user device – and not to the terminal – authenticating the user" (emphasis added). However, the Examiner notes that the underlined portions of applicant's response are not limitations in the claims.

10. Applicant's response (p. 15, ¶3) argues that claim 25 is not obviated by the addition of Daggar. Applicant states the "Daggar simply states that card authenticity must be established. Daggar neither teaches nor suggests how Daggar would establish the authenticity of the card." Applicant's response further argues that the claimed implementation cannot be obviated because "the claim recites the limitations of Claim 12 further comprising authenticating the device to the server." In response, claim 25 does not recite a limitation regarding the method of establishing the card's authenticity. Applicant is directed to col. 13, lines 27-53, where Daggar discloses methods of proving the authenticity of the card (wallet and card micro modules). Applicant is also directed to col. 19, lines 38-60, where Daggar discloses how the digital card is authenticated for secure transactions, such as encrypted PINs and sending them to a digital card issuer. Finally, on p. 16, ¶1, applicant states that none of the references teaches "that the device be

Art Unit: 2134

authenticated, that the server establish a trusted connection with the device and that the server communication terminal authentication information directly to the device along the trusted connection”. As shown above, the device is authenticated, which allows an established trusted connection (as shown in Merritt, Daggar and Manduley) and that terminal authentication information is sent along the trusted connection (Merritt and Manduley). The Examiner notes that applicant’s use of the term “directly” is unnecessary, as this word has been removed from the claims due to its ambiguity.

11. Applicant's response (p. 16, ¶2) argues that claim 12 requires its own authentication component. If applicant intends to rely on a physical component feature, it must be expressly stated in the claims. Further, applicant is directed to Daggar (col. 13, lines 27-53 & col. 19, lines 38-60) where Daggar discloses both methods of proving authenticity and circuitry for performing encryption that allows the recipient trust in the sender.

12. Applicant's response (p. 16, ¶3 – p. 17, ¶1) discusses the term “directly”, however this limitation has been removed from the claims and therefore, the argument is considered moot.

13. Applicant's response (p. 17, ¶1) argues that there exists a “direct connection between the server and the device (Claims 9-26 & 28), without the terminal being involved.” Applicant also states that alternative embodiments teach that the “authenticity output message be conveyed to the terminal, for example when the user device does not have the output capabilities”. However, the use of the term “directly” is ambiguous because it suggests a lack of intervening components, which does not exist when tunneling. Even if, as argued by applicant (p. 17, ¶2), the two connections are distinct, a tunneled connection is not a direct connection. The American Heritage College Dictionary defines *direct* as “Proceeding without interruption in a straight

course or line; not deviating or swerving: a direct route; Having no intervening persons, conditions, or agencies; immediate: direct contact; direct sunlight.” In networking terminology, a direct connection would imply a hardware connection. When a server is connection through the Internet to a web browser, the connection is not without intermediates. The Examiner notes that claim 28 has been cancelled by applicant’s amendment.

14. Applicant's response (p. 18, ¶2 – p. 19, ¶1) is directed to the Examiner’s previous response “[w]hile the information from the user’s card is given to the terminal before authentication, the claims do not state that the terminal must be trusted before the user accesses the terminal.” The Examiner notes that applicants “are not claiming that a terminal must be trusted before it is accessed”, as stated in applicant’s instant response.

15. Applicant's response (p. 19, ¶2) is directed to the Examiner’s previous response “the claims do not recite a limitation where a user is only inclined to enter personal information, such as a pin to the terminal after authentication message has arrived.” The Examiner notes, as stated by applicant, that applicant is only claiming the server and method performed by the server and that applicants believe the patentability of the invention does not hinge on the post-authentication entry of personal information and consequently have not included the claim language to that effect.”

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2134

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

17. Claims 9-11 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,475,756 to Merritt.

Regarding claims 9 and 11, Merritt discloses a server/host (Fig. 1, element 2), a communications component (Fig. 1, element 9), a receiver means (Fig. 3, elements 310 and 360), an authenticity component to verify the terminal's authenticity (Fig. 1, elements 4 and 8, Fig. 3, element 315 and col. 2, lines 10-14) and a message generation component (Fig. 1, element 3) and a storage location (Fig. 1, element 3) for storing a user-specific authenticity output message/PSP (col. 4, lines 11-20).

Regarding claim 10, Merritt discloses the host and the terminal negotiating a session key (col. 6, lines 54-62).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. Claims 12-19, 21, 22 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of U.S. Patent 5,737,423 to Manduley.

Regarding claims 12, 21 & 30, Merritt discloses a server/host authenticating a terminal/ATM (Fig. 3, #315), establishing a first authenticated trusted connection upon success of said authenticating (Fig. 3, #315) which also establishes a second trusted connection between

Art Unit: 2134

the user/device and the server. Merritt further discloses the server authenticating it to the device/user by providing a terminal authenticity message/PSP sent to the terminal to be displayed to the user (second trusted connection) (Fig. 3, #380). Merritt lacks sending the authenticity to the device. The Manduley reference teaches that smart cards are useful in secure transactions, particularly as an electronic purse (as would be used at an ATM) (col. 1, lines 11-29). Manduley also teaches that exchanging messages between a user and a smart card is useful to make sure the correct user is using the smart card (col. 2, lines 7-23 & col. 1, lines 41-56). More specifically, Manduley teaches that the smartcard contains an LCD display that will, at the request of the server/issuing authority, display a message to the user (col. 3, lines 11-16, lines 47-58). This message can be a message requesting the user to enter a response (col. 3, lines 47-58) to authenticate the user's presence (col. 4, lines 7-15). The response is encrypted, thereby authenticating the card (col. 2, lines 7-15 & col. 4, lines 7-13). In this situation, the smart card is acting as a second interface to the server (rather than just a terminal). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send the authenticity output message to the smart card. One of ordinary skill in the art would have been motivated to perform such a modification because smart cards are used in secure transactions and because the legitimate user of the card will be reading the messages, as taught by Manduley (col. 2, lines 7-23 & col. 1, lines 41-56).

Regarding claim 13, Merritt discloses communicating a message to a user (Fig. 5, element 515).

Regarding claims 14, 17 & 19 Merritt discloses a smart card system, as described above, but lacks displaying messages on the card. Manduley teaches that by exchanging a set of

messages between a user and a smart card (col. 2, lines 7-23), one can assure that the user is actually in possession of the card (col. 1, lines 41-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to incorporate a visual display in Merritt's smart card for the purposes of exchanging messages between the user and the card. One of ordinary skill in the art would have been motivated to perform such a modification to ensure that the person responding to a message is actually in possession of the card, as taught by Manduley.

Regarding claim 15, Merritt discloses a terminal displaying a message (col. 3, lines 40-45).

Regarding claim 16, Merritt discloses accessing a database/lookup table that stores user-specific messages/PSPs (col. 7, lines 1-10).

Regarding claim 18, Merritt discloses authentication information contained on the card (col. 3, lines 64-67 and col. 4, lines 1-11) to be read by the terminal/ATM (Fig. 3). Merritt discloses a terminal displaying an authenticity output message/PSP in response to authentication (Fig. 5 and col. 3, lines 20-48).

Regarding claim 22, Merritt discloses a message/PSP taking many forms, such as a still image, a sequence of images, a video or an audio clip (col. 4, lines 16-23).

Regarding claim 26, Merritt discloses authenticating a user (Fig. 3, element 390).

20. Claims 23 & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of Manduley, as applied to claim 21 above, in further view of Schneier. Merritt, as modified above, lacks partially outputting a message. However, Schneier teaches that SKEY is a

Art Unit: 2134

known authentication protocol (as the PSP is used to authenticate the server/host). In SKEY, each entity has a list of numbers (message). One of the numbers is outputted to be recognized by the other entity (partial message) (page 53). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SKEY protocol for authentication using a message/PSP. One of ordinary skill in the art would have been motivated to perform such a modification because an eavesdropper gains no information about the message in that each output of the message is used only once (page 53).

21. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of Manduley, as applied to claim 12 above, in further view of U.S. Patent 4,868,376 to Lessin et al. (Lessin). Merritt discloses a smart card system, as described above, but lacks the card requesting the user authenticate himself. Lessin teaches that by requiring the user enter a PIN, a card can prevent unauthorized access to data (col. 4, lines 7-11 and col. 8, lines 27-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt's smart card system to request the user authenticate himself to prevent unauthorized access. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized access to data on the card, as taught by Lessin.

22. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merritt in view of Manduley, as applied to claim 12 above, in view of U.S. Patent 5,748,737 to Daggar. Merritt discloses a smart card system, as described above, but lacks authenticating the card to the server. Daggar teaches that establishing card authenticity is needed to make sure data from a card is

Art Unit: 2134

genuine and to prevent indiscriminate card reproduction (col. 7, lines 13-19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have Merritt's server authenticate the card to ensure data integrity. One of ordinary skill in the art would have been motivated to perform such a modification to ensure the data from the card is genuine and to prevent indiscriminate card reproduction, as taught by Daggar.

Conclusion

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703) 746-7239 (for formal communications intended for entry)

Or:

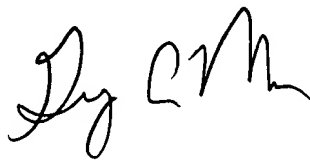
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS
January 7, 2005



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100